

Active Directory-based User Login

Smartcard login policies are also enforced

- DirectControl for OS X supports CAC or PIV smartcard login to Active Directory granting Kerberos tickets for SSO to integrated services
- Users configured for Smartcard interactive login only are not allowed to login with a password, however Kerberos login after smartcard is allowed

Kerberos provides strong mutual authentication to Servers after desktop smartcard login



```
david.mcneely@test-rhel54:~
Using Kerberos authentication
Using principal david.mcneely@CENTRIFY.DEMO
Got host ticket host/test-rhel54.centrify.demo@CENTRIFY.DEMO
login as david.mcneely@CENTRIFY.DEMO
Successful Kerberos connection
*****
NOTICE TO USERS
This computer is the property of Centrify Corp. It is for authorized
Users (authorized or unauthorized) have no explicit or implicit e
rivity.
Any or all uses of this system and all files on this system may b
monitored, recorded, copied, audited, inspected, and disclosed to
trify site and law enforcement personnel, as well as authorized co
er agencies, both domestic and foreign. By using this system, th
to such interception, monitoring, recording, copying, auditing,
disclosure at the discretion of authorized site or Centrify Corp
Unauthorized or improper use of this system may result in adminis
inary action and civil and criminal penalties. By continuing to
you indicate your awareness of and consent to these terms and co
. LOG OFF IMMEDIATELY if you do not agree to the conditions stat
ing.
Centrify policy and rules for computing, including appropriate us
at http://www.centrify.com/termsofuse.asp
*****
Last login: Thu Jul 21 15:58:22 2011 from test-dc2008.centrify.de
[david.mcneely@test-rhel54 ~]$
```

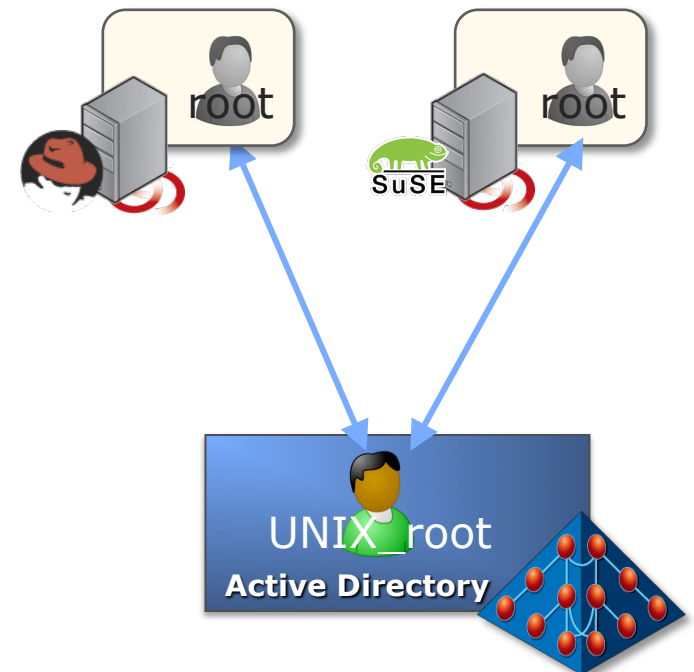
Lock Down Privileged Accounts

Lockdown privileged and service accounts within Active Directory

- Online authentication requires AD-based password validation
- Offline authentication uses the local cached account
- Passwords are synchronized to local storage for single user mode login

Leverage role-based privilege grants to eliminate risks exposed by these accounts

- Eliminating need to access privileged accounts
- Enables locking down these account passwords



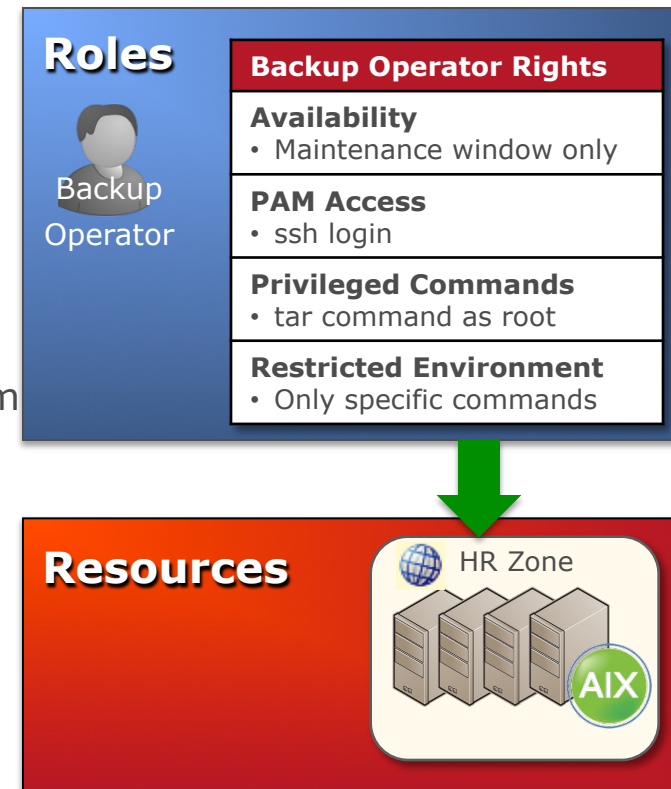
Associate Privileges with Named Individuals

Centralized role-based policy management

- Create Roles based on job duties
- Grant specific access and elevated privilege rights
- Eliminate users' need to use privileged accounts
- Secure the system by granularly controlling how the user accesses the system and what he can do

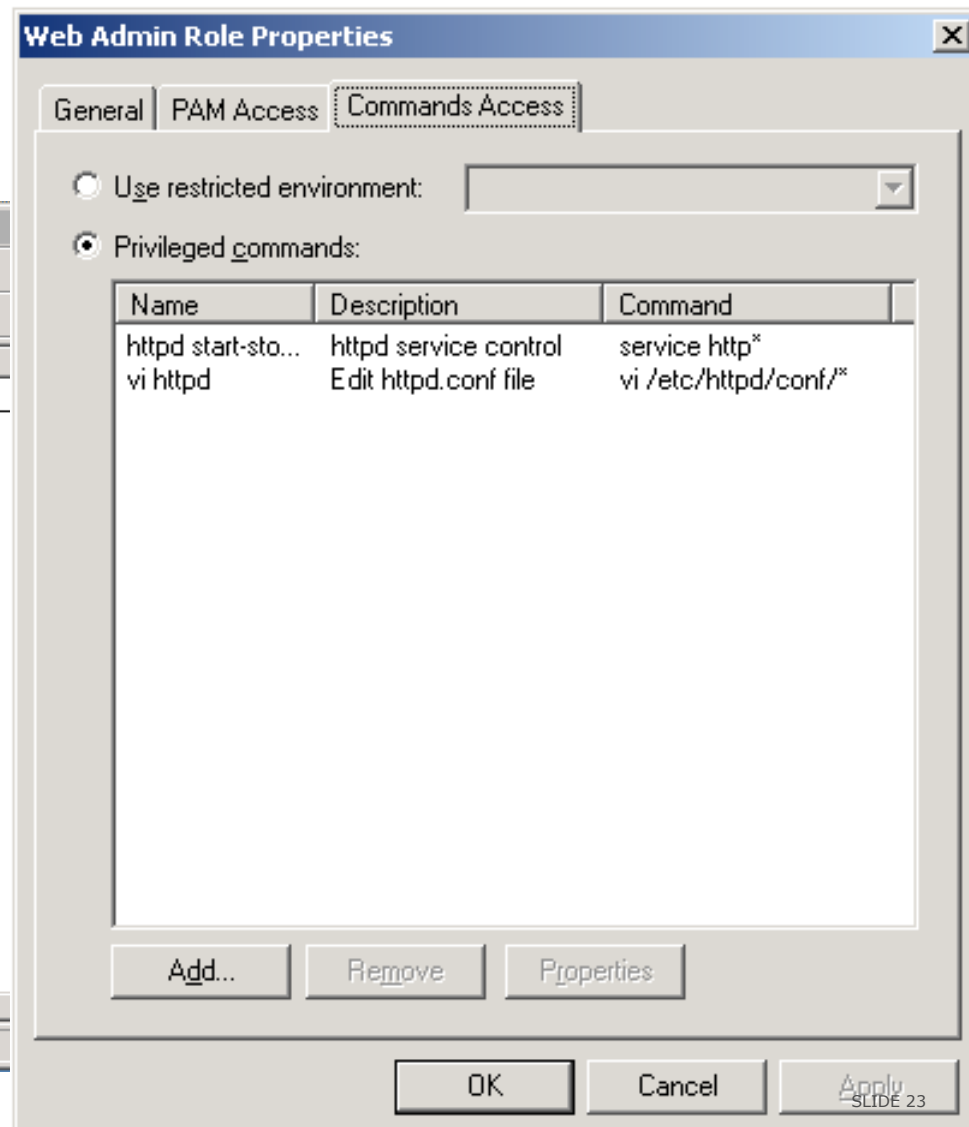
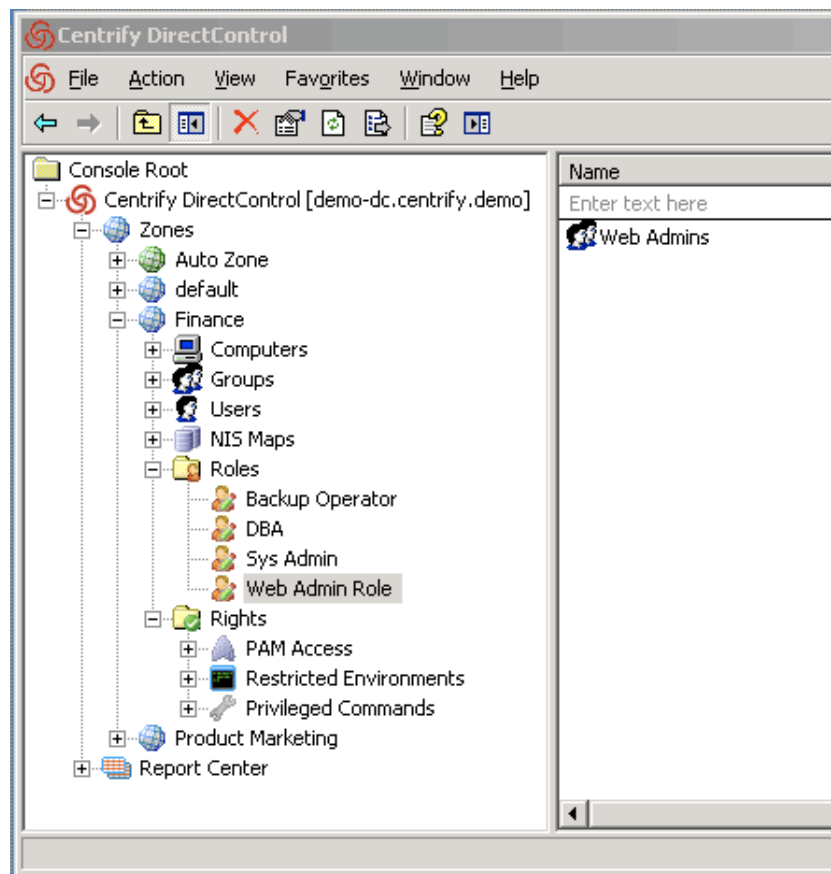
Unix rights granted to Roles

- Availability – controls *when* a Role can be used
- PAM Access – controls *how* users access UNIX system interfaces and applications
- Privilege Commands – grants elevated privileges where needed
- Restricted Shell - controls allowed commands in the user's environment



Grant Privileged Commands to Roles

- Web Admins need root privileges to manage Apache Services



Role Assignments Ensure Accountability

Role Assignment

- Active Directory Users are assigned to a Role, eliminating ambiguity, ensuring accountability
- Active Directory Groups can be assigned to a Role, simplifying management
- User assignment can be date/time limited – enabling temporary rights grants

Assignment Scope

- Roles apply to all computers within a Zone
- Assignment can be defined for a specific Computer



Example: Privilege Access in Current Environment

- Web Admin editing the httpd.conf requires root permissions

User Session

```
[twilson@test-rhel5 ~]$ su root
Password:
[root@test-rhel5 twilson]# vi /etc/httpd/conf/httpd.conf
[root@test-rhel5 twilson]# /sbin/service httpd restart
Stopping httpd:                               [ OK ]
Starting httpd:                               [ OK ]
[root@test-rhel5 twilson]#
```

Security Log (/var/log/secure)

```
Oct 26 10:13:27 test-rhel5 sshd[1786]: pam_unix(sshd:session): session opened for user twilson by (uid=0)
Oct 26 10:14:45 test-rhel5 su: pam_unix(su:session): session opened for user root by (uid=10004)
```

Example: Rights Dynamically Granted at Login

```
[twilson@test-rhel5 ~]$ id
uid=10004(twilson) gid=10001(unixuser) groups=10001(unixuser)
[twilson@test-rhel5 ~]$ adquery group -a "Web Admins"
centrify.demo/Users/Tim Wilson
centrify.demo/Users/David McNeely
[twilson@test-rhel5 ~]$
[twilson@test-rhel5 ~]$ dzinfo
Zone Status: DirectAuthorize is enabled
User: twilson
Forced into restricted environment: No
```

Role Name	Avail	Restricted Env
Web Admin Role	Yes	None

PAM Application	Avail	Source Roles
ftpd	Yes	Web Admin Role
sshd	Yes	Web Admin Role

Privileged commands:			
Name	Avail	Command	Source Roles
vi httpd	Yes	vi /etc/httpd/conf/*	Web Admin Role
httpd	Yes	service http*	Web Admin Role
start-stop-rest			
art			

```
[twilson@test-rhel5 ~]$
```

Example: Privileged Access with Centrify Suite

- Web Admin editing the httpd.conf using DirectAuthorize privilege elevation

User Session

```
[twilson@test-rhel5 ~]$ dzdo vi /etc/httpd/conf/httpd.conf
[twilson@test-rhel5 ~]$ dzdo /sbin/service httpd restart
Stopping httpd:                               [ OK ]
Starting httpd:                               [ OK ]
[twilson@test-rhel5 ~]$
```

Security Log (/var/log/secure)

```
Oct 26 10:25:42 test-rhel5 sshd[1786]: pam_unix(sshd:session): session opened for user twilson by (uid=0)
Oct 26 10:26:03 test-rhel5 dzdo: twilson : TTY=pts/5 ; PWD=/home/twilson ; USER=root ; COMMAND=/bin/vi /
etc/httpd/conf/httpd.conf
Oct 26 10:28:27 test-rhel5 dzdo: twilson : TTY=pts/5 ; PWD=/home/twilson ; USER=root ; COMMAND=/sbin/
service httpd restart
```


Leveraging Active Directory as Centralized Security Infrastructure

AUDIT ACTIVITIES

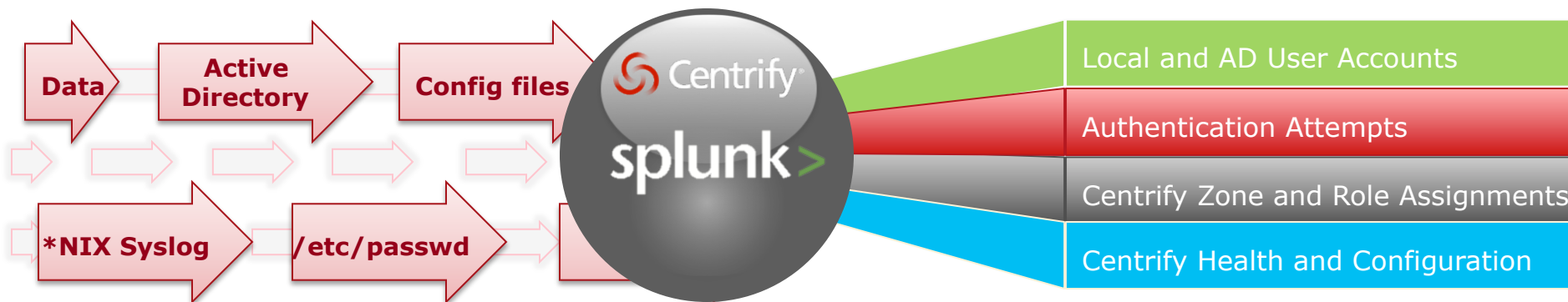
System Logs and Events Provide Limited Visibility

Show me accounts not used in last 90 days.

Are there any systems where Centrify is not connected?

How long was a user in a role?

- Syslog rollup brings in operational intelligence from other systems, apps, SIEM, security devices, etc.



Metrics and Alerts

Local and AD User Accounts
Authentication Attempts
Centrify Zone and Role Assignments
Centrify Health and Configuration

Dashboards and Reports

I want to see all failed login attempts.

Are there any newly created local accounts on my server?

Who zone-enabled this user?

- Shows changes in AD, *nix login attempts, Windows login attempts, Centrify agent health, etc.

For Monitoring and Reporting of Logged Changes

The screenshot displays the Splunk Enterprise web interface. The top navigation bar includes links for Dashboards, Logs and Configs, Search, Support, Help, and About. The main content area is divided into two columns.

Centrify Insight Overview

Getting Started

Add the data sources required for this app to provide meaningful functionality:

- Splunk Search Head — Install Splunk 4.2, install this app, [enable the twitter input](#) and forward the remaining boxes here.
- Windows Domain Controller(s) — Install the Windows Universal Forwarder. Collect Security Log and Active Directory. Must be run as an Active Directory domain user.
- Centrify managed *NIX boxes — Install Splunk 4.2, install this app, [enable the appropriate inputs](#) and forward to the Splunk Search Head.

To learn more about this app and Centrify:

- [Read the Installation Guide](#)
- [Free Active Directory Tools for UNIX, Linux and Mac](#)
- [Centrify Express Community](#)
- [Splunk Answers for Centrify Insight](#)
- [Centrify Customer Support](#)
- [Centrify Support Tweets](#)

NOTE: There are several scheduled searches we run on a regular basis in Splunk Enterprise. In Splunk Free you will need to manually run these searches once or twice a day. It is also useful to manually run these searches after changes like turning on addebug to collect centrifydc.log data.

- [Reload centrifydc.log hosts](#)
- [Reload centrifydc.log modules](#)
- [Reload Active Directory Lookups](#)

Recent Centrify Support Tweets

date ↕	tweet ↕
about a month ago	adinfo adds a capability to validate AD user and password against a given domain. E.g., adinfo -A -u ADUSERNAME I
about a month ago	Centrify Suite 2011 now integrates more than 280 UNIX, Linux and Mac platforms with Microsoft Active Directory.
about a month ago	Centrify Suite 2011 now available for download. For more details, visit http://bit.ly/hLcvok (Requires login to Centrify S
about a month ago	@pwylu : Did you mean SLES 11 SP1 ? If so 'yes'. Please check out our detailed list of supported platforms here: http://bit.ly/bYtSc6
about a month ago	RT @CentrifyNews: Happy 6 year birthday #Centrify #DirectControl !! http://bit.ly/bYtSc6 V1.0 had support for only

Search Active Directory and Zones

Object Type: Group Activity Type: Altered Membership Group Type: Global Distribution Search Text: employees

≥ 2 matching events | 43,097 scanned events

Employees

Added member(s) to this group about a minute ago by TANGOIT

tango.se/Users/Employees

AD Group	Group Scope	Group Type	Mail	Affected Members
Employees	Global	Distribution	employees@tango.se	tango.se/Users/Alpha tango.se/Users/Bravo tango.se/Users/Charlie

Show all 264 lines for 8 events DC — WIN-D64N2IVJ19B.tango.se Windows Event Codes — 4750, 4751, 5136

Employees

Added member(s) to this group 3 days ago by TANGOIT

tango.se/Users/Employees

AD Group	Group Scope	Group Type	Mail	Affected Members
Employees	Global	Distribution	employees@tango.se	tango.se/Users/David Twamley

Show all 88 lines for 3 events DC — WIN-D64N2IVJ19B.tango.se Windows Event Codes — 4750, 4751

High Definition Visibility Provided by Session Recording

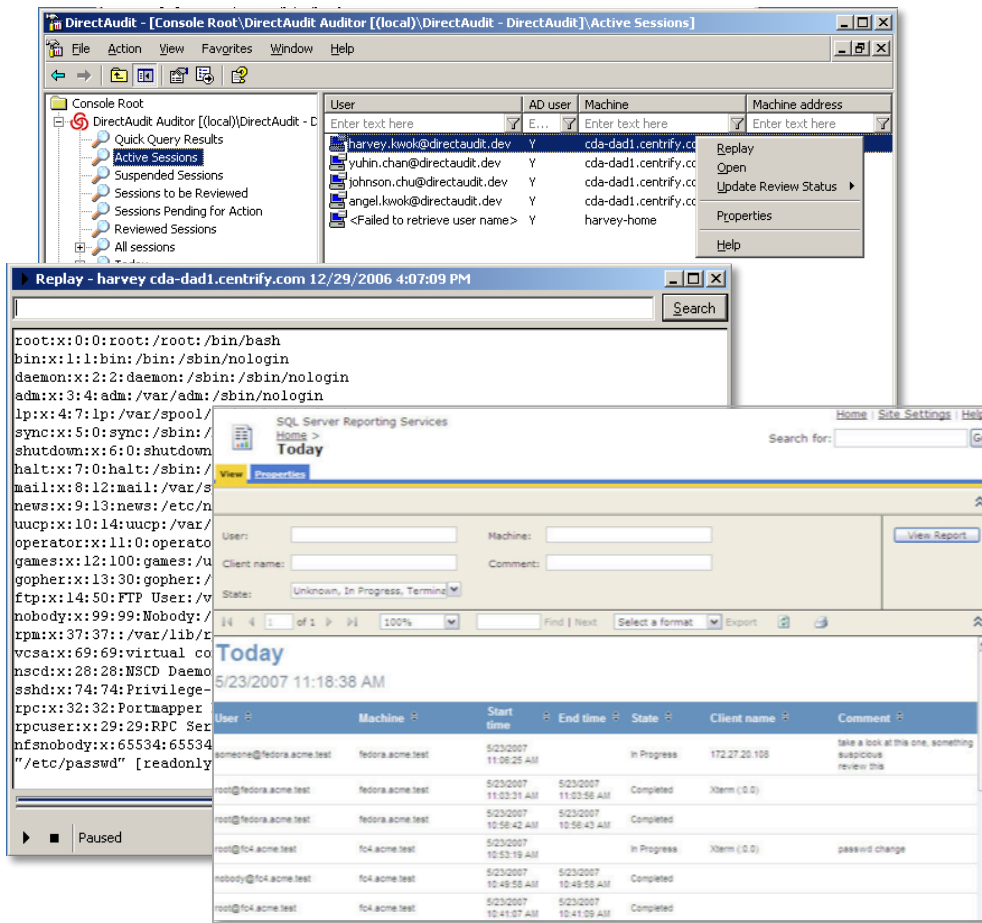
UNIX system access & activity is linked to users' unique AD account

Tracks all user access to systems

- Provides full user session replay
- Shows what commands were executed
- Shows what changes they made to key files

Centrally search captured sessions
for events, such as:

- All accesses to sensitive files
- Any execution of shutdown or kill
- All su and sudo executions



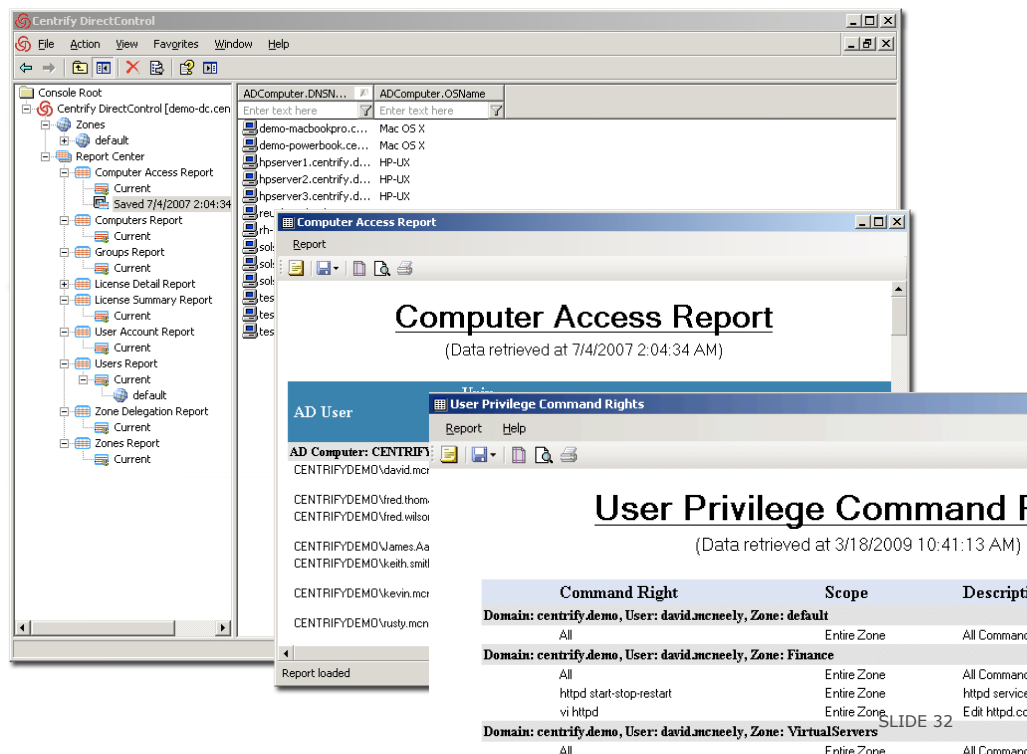
Reporting Simplified with Centralized Management

Authorization and Access Reports can be centrally created:

- Reporting on user account properties
- Detailing user role assignments and privilege command rights
- Showing user access rights to computers

Active Directory based reporting

- Reports are generated on live, editable AD information
- Administrators can take snapshots of a report



The image displays two screenshots of the Centrify DirectControl application. The top screenshot shows the 'Computer Access Report' window, which lists various computers and their operating systems. The bottom screenshot shows the 'User Privilege Command Rights' window, which displays a table of command rights for a specific user.

Computer Access Report
(Data retrieved at 7/4/2007 2:04:34 AM)

AD User	AD Computer: CENTRIFY
CENTRIFY\DEMO\david.mcr	
CENTRIFY\DEMO\fred.thom	
CENTRIFY\DEMO\fred.wilson	
CENTRIFY\DEMO\James.Aa	
CENTRIFY\DEMO\keith.smil	
CENTRIFY\DEMO\kevin.mcr	
CENTRIFY\DEMO\rusty.mcn	

User Privilege Command Rights
(Data retrieved at 3/18/2009 10:41:13 AM)

Command Right	Scope	Description
Domain: centrify.demo, User: david.mcneely, Zone: default		
All	Entire Zone	All Command
Domain: centrify.demo, User: david.mcneely, Zone: Finance		
All	Entire Zone	All Command
httpd start-stop-restart	Entire Zone	httpd service
vi httpd	Entire Zone	Edit httpd.co
Domain: centrify.demo, User: david.mcneely, Zone: VirtualServers		
All	Entire Zone	All Command

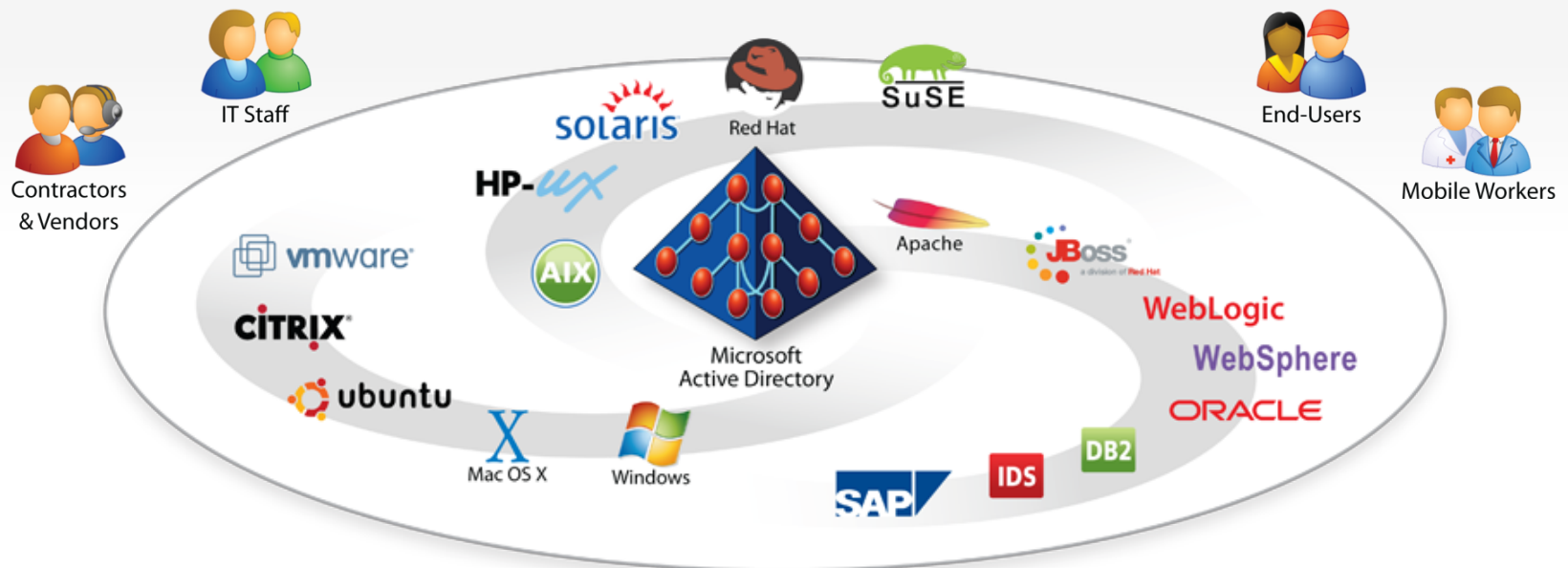
Addressing NIST 800-53 for UNIX

NIST SP 800-53 Requirement	Leverage Active Directory to:
Identity & Authentication (IA) <ul style="list-style-type: none">Uniquely identify and authenticate usersEmploy multifactor authentication	<ul style="list-style-type: none">Link entitlements and actions to a centrally managed user identity in ADSupport smartcard authentication for Mac Workstations
Access Control (AC) <ul style="list-style-type: none">Restrict access to systems and to privilegesEnforce separation of duties and least-privilege rights management	<ul style="list-style-type: none">Enforce centralized policies for Role-based access and privilege rightsEnforce administrative separation of duties
Audit & Accountability (AU) <ul style="list-style-type: none">Capture in sufficient detail to establish what occurred, the source, and the outcome	<ul style="list-style-type: none">Capture all interactive sessions on audited systems, attributing the actions to the accountable personProvide search and session replay
Configuration Management (CM) <ul style="list-style-type: none">Develop/maintain a baseline configurationAutomate enforcement for access restrictions and audit the actions	<ul style="list-style-type: none">Automatically enforce a baseline security policyContinuously enforce/update the security policy
Systems & Communications (SC) <ul style="list-style-type: none">Boundary ProtectionTransmission Integrity and ConfidentialityCryptographic Key Establishment and Management including PKI Certificates	<ul style="list-style-type: none">Enforce domain and group-based isolation policies to protect sensitive assetsEncrypt data in motion between systemsAutomate PKI management and validation on protected systems

The Centrify Vision

Control, Secure and Audit Access to Cross-Platform Systems and Applications

Centrify the Enterprise



Leverage infrastructure you already own – Active Directory – to:

Control

What users can access

Secure

User access and privileges

Audit

What the users did

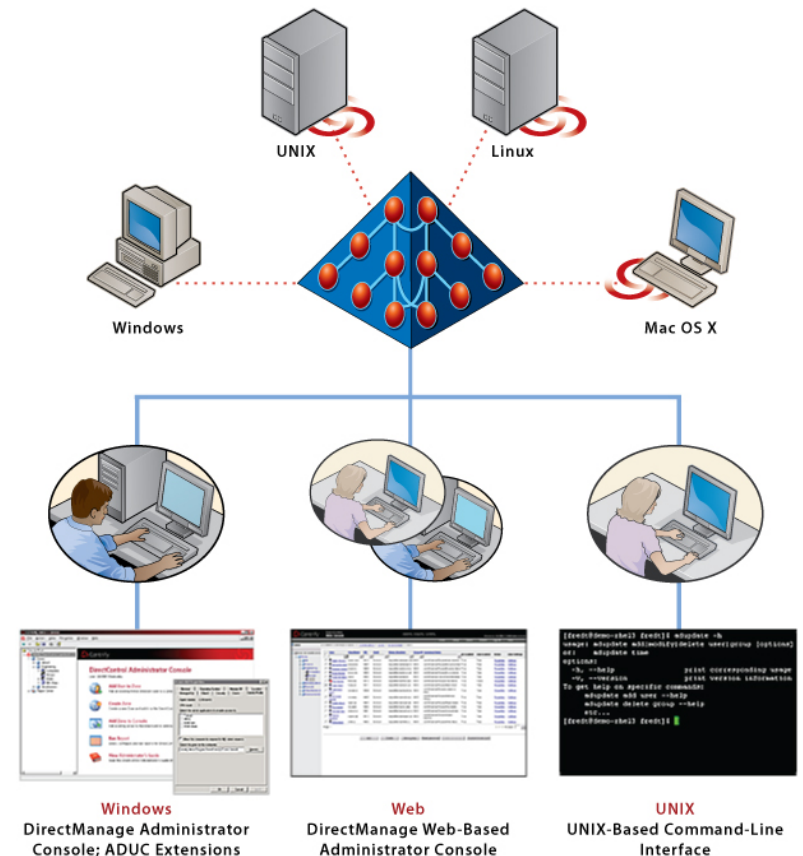
Reduce Costs Through Identity Consolidation

"Islands of identity" need to be managed and secured

- Locally managed etc/passwd file
- Legacy NIS or hand-built scripting
- High cost & inefficient to maintain

With Centrify:

- ✓ Consolidate disparate UNIX and Linux identity stores into AD
- ✓ Implement least-privilege security
- ✓ Centrally enforce security and configuration policies across UNIX, Linux and Mac systems
- ✓ Instantly terminate access to all systems and applications centrally



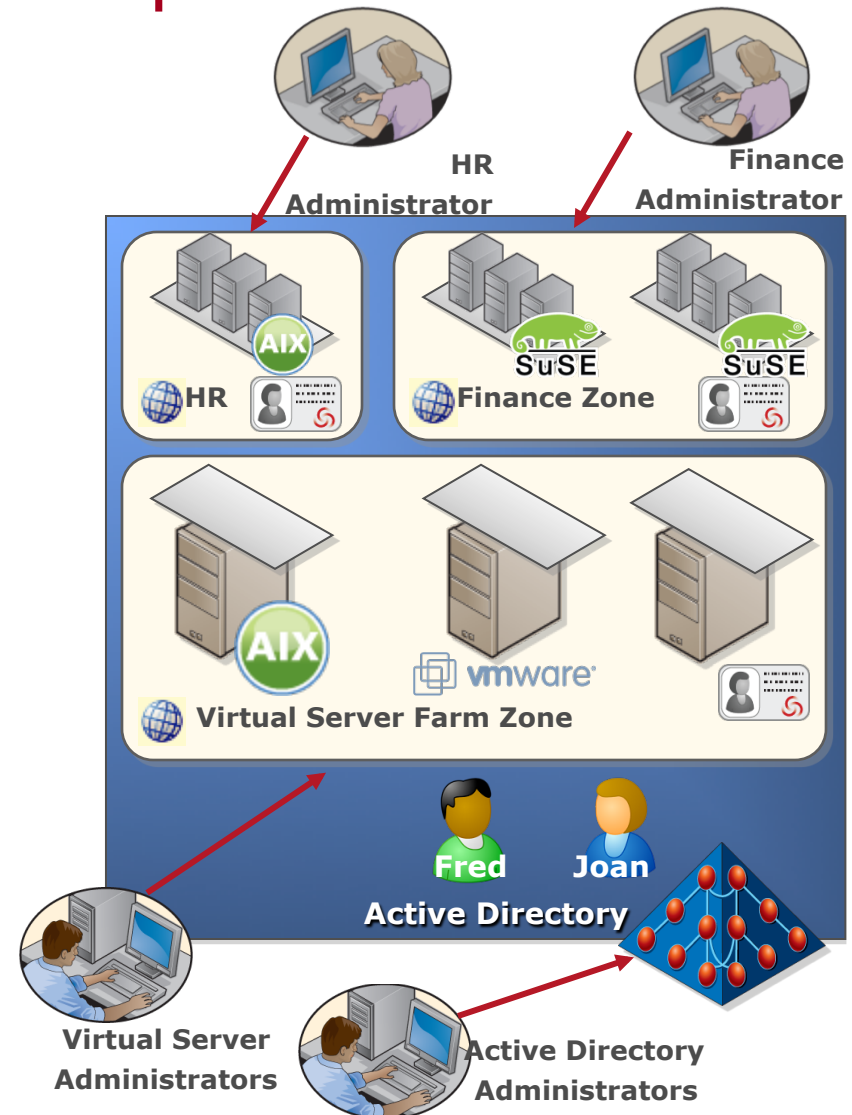
Mitigate Risks & Address Compliance

Evolving threat landscape and regulatory environment

- Shared “root” password compromises security & exposes intellectual property
- Anonymous access...
- Audits require reporting that ties access controls and activities to individuals

With Centrify:

- ✓ Associate privileges with individuals
- ✓ Lock down privileged accounts
- ✓ Enforce separation of duties
- ✓ Isolate sensitive systems
- ✓ Protect data-in-motion
- ✓ Audit all activity



Why Customers Choose Centrify

Gartner Centrify is the "right vendor to choose" for Active Directory integration: Centrify's solution is "mature, technically strong, full featured, and possess(es) broad platform support." – 2009

"We recommended that clients strongly consider Centrify ... its products can fit well within a multivendor IAM portfolio." – 2010

Experience & Expertise

- 3500+ enterprise customers
- Largest dedicated team
- Unparalleled 24x7 support
- Record growth and profitable

The Best Solution

- Single architecture based on AD
- Comprehensive suite
- Proven success in deployments
- Non-intrusive

Industry Awards



Industry Certifications



Learn More and Evaluate Centrify Yourself

WEB SITE

www.centrify.com

FEDERAL SOLUTIONS

www.centrify.com/federal

TECHNICAL VIDEOS & MORE

www.centrify.com/resources

SUPPORTED PLATFORMS

www.centrify.com/platforms

REQUEST AN EVAL

www.centrify.com/trial

FREE SOFTWARE

www.centrify.com/express

CONTACT US

www.centrify.com/contact

PHONE

Worldwide: **+1 (408) 542-7500**

Europe: **+44 (0) 1344 317950**